2.6 INFORMATION SYSTEMS SECURITY STANDARDS

2.6.1 Introduction

2.6.1.1 Purpose

This section provides the information system security standards necessary to implement security at the required level of protection.

2.6.1.2 Scope

The standards mandated in this section apply to all DoD information technology systems. This section provides the security standards applicable to information processing, transfer, modeling and standards, and Human-Computer Interfaces (HCI). This section also addresses standards for security audit and key management mechanisms. Subsection 2.6.2 addresses mandated security standards, and subsection 2.6.3 addresses emerging security standards.

2.6.1.3 Background

The Technical Architecture Framework for Information Management (TAFIM) provides a blueprint for the Defense Information Infrastructure (DII), capturing the evolving vision of a common, multipurpose, standards-based technical infrastructure. The DoD Goal Security Architecture (DGSA), Volume 6 of the DoD TAFIM, dated 30 April 1996, provides a comprehensive view of the architecture from the security perspective. The DGSA is a generic architectural framework for developing mission-specific security architectures; it includes security services for information systems (authentication, access control, data integrity, data confidentiality, non-repudiation, and availability). Although advancements in security theory and technology are needed to develop systems that are consistent with DGSA, the DGSA concepts and principles can be incorporated into current systems.

Interoperability requires seamless information flow at all levels of information classification without compromising security. The goal is to protect information at multiple levels of security, recognizing that today's DoD systems are "islands" of system-high solutions.

Systems that process sensitive data must be certified and accredited before use. Certification is the technical evaluation of security features and other safeguards, made in support of the accreditation. Accreditation is the authorization by the Designated Approving Authority (DAA) that an information system may be placed into operation. By authorizing a system to be placed in operation, the DAA is declaring that the system is operating under an "acceptable level of risk." Therefore, system developers should open dialog with the Certifier and DAA concurrently with their use of the Joint Technical Architecture (JTA), as DAA decisions can affect the applicability of standards within specific environments.

DoD systems should have adequate safeguards to enforce DoD security policies and system security procedures. System safeguards should provide adequate protection from user attempts to circumvent system access control, accountability, or procedures for the purpose of performing unauthorized system operations.

Security requirements and engineering should be determined in the initial phases of design. The determination of security services to be used and the strength of the mechanisms providing the services are primary aspects of developing the specific security architectures to support specific domains. Section 2.6 of the JTA is used after operational architectural decisions are made regarding the security services needed and the required strengths of protection of the mechanisms providing those services.

The proper selection of standards can also provide a basis for improved information protection. Although few specific standards for the general topic of "information protection" exist within Defensive Information Warfare, selecting standards with security-relevant content contributes to the overall improvement of the security posture of information systems.

2.6.2 Mandates

This subsection identifies the mandatory standards, profiles, and practices for information systems security standards. Each mandated standard or practice is clearly identified on a separate line, and includes a formal reference that can be included within Requests for Proposals (RFP) or Statements of Work (SOW). Appendix B contains a table that summarizes the mandated standards from this section, as well as providing information on how to obtain the standards.

2.6.2.1 Introduction

This section contains the mandatory information systems security standards and protocols that shall be implemented in systems that have a need for the corresponding interoperability-related services. If a service is to be implemented, then it shall be implemented at the required level of protection using the associated security standards in this section. If a service is specified by more than one standard, the appropriate standard should be selected based on system requirements. Section 2.6.2 is structured to mirror the overall organization of the JTA so that readers can easily link security topics with the related subject area in the sections of the JTA (information processing; information transfer; information modeling, metadata, and information exchange; and human-computer interface) and their subsections.

2.6.2.2 Information Processing Security Standards

Technical evaluation criteria to support information system security policy, and evaluation and approval, disapproval, and accreditation responsibilities are promulgated by DoD Directive (DoDD) 5200.28. Based on the required level of trust, the following information processing security standards are mandated.

2.6.2.2.1 Application Software Entity Security Standards

The following standards are mandated for the development and acquisition of application software consistent with the required level of trust:

- DoD 5200.28-STD, The DoD Trusted Computer System Evaluation Criteria, December 1985.
- NCSC-TG-021, Version 1, Trusted Database Management System Interpretation, April 1991.

If FORTEZZA services are used, the following are mandated:

- FORTEZZA Application Implementers' Guide, MD4002101-1.52, 5 March 1996.
- FORTEZZA Cryptologic Interface Programmers' Guide, MD4000501-1.52, 30 January 1996.

2.6.2.2.2 Application Platform Entity Security Standards

For the application platform entity, security standards are mandated for data management services and operating system services. Security is an important part of other application platform service areas, but there are no standards for the other service areas.

2.6.2.2.2.1 Data Management Services

The following standard is mandated for data management services consistent with the required level of trust:

- NCSC-TG-021, Version 1, Trusted Database Management System Interpretation, April 1991.

2.6.2.2.2.2 Operating System Services Security

For the application platform entity, the following standard is mandated for the acquisition of operating systems consistent with the required level of trust:

- DoD 5200.28-STD, The DoD Trusted Computer System Evaluation Criteria, December 1985.

2.6.2.2.2.2.1 Security Auditing and Alarms Standards

Security auditing is a review or examination of records and activities to test controls, ensure compliance with policies and procedures, detect breaches in security, and indicate changes in operation. Security alarm

reporting is the capability to receive notifications of security-related events, alerts of any misoperations of security services and mechanisms, alerts of attacks on system security, and information as to the perceived severity of any misoperation, attack, or breach of security.

The following standard is mandated for security auditing or alarm reporting:

- DoD 5200.28-STD, The DoD Trusted Computer System Evaluation Criteria, December 1985.

2.6.2.2.2.2.2 Authentication Security Standards

Authentication supports tracing security-relevant events to individual users. If Open Software Foundation DCE Version 1.1 is used, the following authentication standard is mandated:

- IETF RFC-1510, The Kerberos Network Authentication Service, Version 5, 10 September 1993.

If DCE Version 1.1 is not used, the following authentication standard is mandated:

- FIPS-PUBS 112, Password Usage, 30 May 1985.

Additional guidance documents: NCSC-TG-017 - A Guide to Understanding Identification and Authentication in Trusted Systems; CSC-STD-002 - DoD Password Management Guidance.

2.6.2.3 Information Transfer Security Standards

This section discusses the security standards that shall be used when implementing information transfer security services. Security standards are mandated for the following information transfer areas: end system (host standards), and network (internetworking standards).

2.6.2.3.1 End-system Security Standards

Security standards for host end-systems are included in the following subsections.

2.6.2.3.1.1 Host Security Standards

Host end system security standards include security algorithms, security protocols, and evaluation criteria. The first generation FORTEZZA Cryptographic Card is designed for protection of information in messaging and other applications.

For systems required to interface with Defense Message System, the following standard is mandated:

- FORTEZZA Interface Control Document, Revision P1.5, 22 December 1994.

2.6.2.3.1.1.1 Security Algorithms

To achieve interoperability, products must support a common transport protocol. Transport protocols must agree on a common cryptographic message syntax, cryptographic algorithms, and modes of operations (e.g., cipher block chaining). Transport protocols support negotiation mechanisms for selecting common syntax, algorithms, and modes of operation.

The following paragraphs identify security standards that shall be used for the identified types of cryptographic algorithms.

Message digest or hash algorithms are one-way functions which create a "fingerprint" of a message. They provide data integrity when used in conjunction with other cryptographic functions. If message digest or hash algorithms are required, Key Recovery will be implemented in the certificate management hierarchy. The NSA developed encryption algorithm SKIPJACK is mandated:

- SKIPJACK, NSA, R21-TECH-044, 21 May 1991.

Digital signatures provide strong identification and authentication. Related standards include public key certificate standards (X.509) and directory service standards (X.500). If digital signature is required, the following standard is mandated:

- FIPS PUB 186, Digital Signature Standard, May 1994.

Encryption prevents unauthorized disclosure of information during transmission. Systems processing classified information must use a Type 1 NSA-approved encryption product, which can also be used to encrypt sensitive but unclassified information.

Key exchange algorithms allow two parties to exchange encryption keys without relying on out-of-band communications. In FORTEZZA applications, the following NSA-developed Type II key exchange algorithm is mandated:

- Key Exchange Algorithm, NSA, R21-TECH-23-94, 12 July 1994.

2.6.2.3.1.1.2 Security Protocols

The following standard is mandated for DoD systems that are required to exchange security attributes, for example sensitivity labels:

- MIL-STD-2045-48501, Common Security Label, 25 January 1995.

Establishment of a certificate and key management infrastructure for digital signature is required for the successful implementation of the security architecture. This infrastructure is responsible for the proper creation, distribution, and revocation of end users' public key certificates. The following standard is mandated:

- ITU-T Rec. X.509 (ISO/IEC 9594-8.2), Version 3, The Directory: Authentication Framework, 1993.

The Message Security Protocol (MSP) Version 4.0 has been revised to accommodate, in part, Allied requirements. All of MSP 4.0 features have been incorporated into ACP-120, Allied Communications Publication 120, Common Security Protocol. The following messaging security protocol is mandated for DoD message systems that are required to exchange sensitive but unclassified and classified information:

- ACP-120, Allied Communications Publication 120, Common Security Protocol, CSP, 1997.

The following key management protocol is mandated:

- SDN.903, revision 3.2, Secure Data Network System (SDNS) Key Management Protocol (KMP), 1 August 1989.

2.6.2.3.1.1.3 Evaluation Criteria Security Standards

The following standards are mandated consistent with the required level of trust:

- DoD 5200.28-STD, The DoD Trusted Computer System Evaluation Criteria, December 1985.
- NCSC-TG-005, Version 1, Trusted Network Interpretation, July 1987.

2.6.2.3.2 Network Security Standards

Systems processing classified information must use Type 1 NSA-approved encryption products to provide both confidentiality and integrity security services within the network.

When network layer security is required, the following security protocol is mandated:

- SDN.301, Revision 1.5, Secure Data Network System (SDNS) Security Protocol 3 (SP3), 1989.

The following standard is mandated for DoD systems that are required to exchange security attributes, for example sensitivity labels:

- MIL-STD-2045-48501, Common Security Label, 25 January 1995.

2.6.2.3.3 Transmission Media Security Standards

There are currently no security standards mandated for transmission media.

2.6.2.4 Information Modeling, Metadata, and Information Security Standards

At this time, no information modeling, metadata, and information security standards are mandated. Process models and data models produced should be afforded the appropriate level of protection. (Ref: NCSC-TG-010, October 1992, A Guide to Understanding Security Modeling in Trusted Systems).

2.6.2.5 Human-Computer Interface Security Standards

DoD 5200.28-STD, DoD Trusted Computer System Evaluation Criteria (TCSEC), December 1985, specifies the minimal security requirements associated with a required level of protection for DoD automated systems. HCI security-related requirements may include authentication, screen classification display, and management of access control workstation resources.

For systems employing graphical user interfaces, the following guideline is mandated:

- DoD Human-Computer Interface Style Guide, TAFIM Version 3.0, Volume 8, 30 April 1996.

2.6.3 Emerging Standards

The standards listed in this subsection are expected to be elevated to mandatory status when implementations of the standards mature.

2.6.3.1 Introduction

The emerging security standards described in this section are drawn from work being pursued by ISO, IEEE, IETF, Federal standards bodies, and consortia such as the Object Management Group (OMG). Section 2.6.3 is structured to mirror the overall organization of the JTA so that readers can easily link security topics with the related subject area in the sections of the JTA (information processing; information transfer; information modeling, metadata, and information exchange; and human-computer interface) and their subsections.

2.6.3.2 Information Processing Security Standards

Information processing security standards are emerging in applications software and application platform entity areas.

2.6.3.2.1 Application Software Entity Security Standards

Emerging application software entity standards include evaluation criteria and World Wide Web (WWW) security-related standards.

2.6.3.2.1.1 Evaluation Criteria Security Standards

The Evaluation Criteria for Information Technology Security (Common Criteria) represents the outcome of efforts to develop criteria for evaluation of IT security that are widely useful within the international community. It is an alignment and development of a number of the existing European, US. and Canadian criteria (ITSEC, TCSEC and CTCPEC respectively). The Common Criteria resolves the conceptual and technical differences between the source criteria. It is a contribution to the development of an international standard, and opens the way to worldwide mutual recognition of evaluation results (ISO/IEC JTC1/SC27/WG3 N304, 23 April 1996).

2.6.3.2.1.2 World Wide Web Security Standards

"The Transport Layer Security (TLS) Protocol, Version 1.0," Tim Dierks (Consensus Development), Christopher Allen (Consensus Development), 21 May 1997, draft-ietf-tls-protocol-03.txt, which incorporates the Secure Sockets Layer (SSL) Protocol Version 3.0, 18 November 1996, is an Internet Engineering Task Force (IETF) Draft document supporting WWW security, and is being considered for standardization. The TLS protocol provides communications privacy over the Internet. The protocol allows

client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. TLS runs above the transport layer.

2.6.3.2.2 Application Platform Entity Security Standards

For the application platform entity, security standards are emerging for software engineering, operating systems, and distributed computing services.

2.6.3.2.2.1 Software Engineering Services Security

For software engineering services, security standards are emerging for Generic Security Service (GSS)-Application Program Interface (API) and POSIX areas.

2.6.3.2.2.1.1 Generic Security Service (GSS)-Application Program Interface (API) Security

The GSS-API, as defined in RFC-1508, September 1993 (IETF), provides security services to callers in a generic fashion, supportable with a range of underlying mechanisms and technologies and hence allowing source-level portability of applications to different environments. RFC-1508 defines GSS-API services and primitives at a level independent of underlying mechanism and programming language environment. RFC-2078, "GSS-API, Version 2.0," J. Linn, January 1997, revises RFC-1508, making specific, incremental changes in response to implementation experience and liaison requests.

The IETF Draft, "Independent Data Unit Protection Generic Security Service Application Program Interface (IDUP-GSS-API)," C. Adams, 25 March 1997, draft-ietf-cat-idup-gss-07.txt, extends the GSS-API (RFC-1508) for non-session protocols and applications requiring protection of a generic data unit (such as a file or message) in a way which is independent of the protection of any other data unit and independent of any concurrent contact with designated "receivers" of the data unit. An example application is secure electronic mail where data needs to be protected without any on-line connection with the intended recipient(s) of that data. Subsequent to being protected, the data unit can be transferred to the recipient(s) – or to an archive - perhaps to be processed as unprotected days or years later.

2.6.3.2.2.1.2 POSIX Security Standards

The following draft IEEE standards define a standard interface and environment for POSIX-based computer operating systems that require a secure environment:

- IEEE P1003.1e, POSIX Part 1: System API - Protection, Audit, and Control Interfaces [C Language], Draft, 16 June 1997.
- IEEE P1003.2c, POSIX Part 2: Shell and Utilities - Protection and Control Interfaces, Draft, 16 June 1997.

These draft standards define security interfaces to open systems for access control lists, audit, privilege, mandatory access control, and information label mechanisms and are stated in terms of their C bindings.

2.6.3.2.2.2 Operating System Services Security

Operating system services security standards are emerging in the following areas: evaluation criteria and authentication.

2.6.3.2.2.2.1 Evaluation Criteria Security Standards

See Section 2.6.3.2.1.1 for a description of the emerging Common Criteria. It is expected that the evolving Common Criteria Protection Profiles will replace those references to the Orange Book (e.g., Orange Book Class C2 would equate to a specific Common Criteria Protection Profile). More information on Common Criteria Protection Profiles is available on NIST's World Wide Web home page at:

http://csrc.nist.gov/nistpubs/cc

2.6.3.2.2.2.2 Authentication Security Standards

IETF RFC-1938, "A One-Time Password System," May 1996, provides authentication for system access (login), and other applications requiring authentication, that is secure against passive attacks based on replaying captured reusable passwords. The One-Time Password System evolved from the S/KEY One-Time Password System that was released by Bellcore.

When Remote Dial In Authentication is required, the following standard may be used:

– IETF RFC 2138, “Remote Authentication Dial In User Service (RADIUS),” April 1997.

2.6.3.2.2.3 Distributed Computing Services Security Standards

DCE Authentication and Security Specification (P315) is a draft Open-Group Specification for DCE.

The Common Object Request Broker Architecture (CORBA) Security Services define a software infrastructure that supports access control, authorization, authentication, auditing, delegation, non-repudiation, and security administration for distributed object-based systems. This infrastructure can be based on existing security environments and can be used with existing permission mechanisms and login facilities. The key security functionality is confined to a trusted core that enforces the essential security policy elements. Since the CORBA Security Services are intended to be flexible, two levels of conformance may be provided. Level 1 provides support for a default system security policy covering access control and auditing. Level 1 is intended to support applications that do not have a default policy. Level 2 provides the capability for applications to control the security provided at object invocation and also for applications to control the administration of an application-specific security policy. Level 2 is intended to support multiple security policies and to provide the capability to select separate access control and audit policies.

2.6.3.3 Information Transfer Security Standards

Security standards are emerging for the following information transfer areas: end-systems (host standards) and network (internetworking standards).

2.6.3.3.1 End-system Security Standards

Emerging end-system security standards include host standards discussed in the following subsection.

2.6.3.3.1.1 Host Security Standards

Security standards are emerging for host end systems in the security protocols and public key infrastructure areas discussed in the following subsections.

2.6.3.3.1.1.1 Security Protocols

In mid-1996, some significant improvements were proposed to the Secure/Multipurpose Internet Mail Extensions (S/MIME) messaging security protocol and the underlying encapsulation protocol, PKCS#7. With these improvements, S/MIME will provide a business quality security protocol for both the Internet and X.400 messaging environments. The improvements include: (1) algorithm independence; (2) support for digitally signed receipts; (3) support for mail lists; and (4) support for sensitivity labels in signed and unsigned/encrypted messages. This effectively merges S/MIME and Message Security Protocol (MSP) 4.0/ACP-120. In November 1997, the IETF formed the S/MIME security protocol working group to create Internet standards based on S/MIME and these improvements.

It is expected that the Trusted Systems Interoperability Group (TSIG) Trusted Information for Exchange for Restricted Environments (TSIX (RE) 1.1) will adopt MIL-STD-2045-48501 as a replacement for its Common Internet Protocol Security Options (CIPSO) labeling standard.

The following are emerging standards for Local Area Network (LAN) security: IEEE 802.10c/D13, Standard for Interoperable LAN Security-Part C: Key Management, and IEEE 802.10g/D7, Secure Data Exchange Label, 1995.

2.6.3.3.1.1.2 Public Key Infrastructure Security Standards

FIPS PUB 196, Entity Authentication Using Public Key Cryptography, 18 February 1997, is based on ISO/IEC 9798-3: 1993, Entity Authentication Using a Public Key System and will provide a standard for Public Key Cryptographic Entity Authentication Mechanisms for use in public key-based challenge-response and authentication systems at the application layer within computer and digital telecommunications systems.

2.6.3.3.2 Network Security Standards

Emerging network standards are listed in Section 2.6.3.3.2.1.

2.6.3.3.2.1 Internetworking Security Standards

RFC-1825, "Security Architecture for the Internet Protocol," R. Atkinson, August 1995, describes the security mechanisms for IP version 4 (IPv4) and IP version 6 (IPv6) and the services that they provide. Each security mechanism is specified in a separate document. RFC-1825 also describes key management requirements for systems implementing those security mechanisms. It is not an overall Security Architecture for the Internet, but focuses on IP-layer security.

The Internet Draft "IP Authentication Header (AH)," Stephen Kent (BBN Corp.), Randall Atkinson (@Home Network), 30 May 1997, draft-ietf-ipsec-auth-05.txt, describes a mechanism for providing cryptographic authentication for IPv4 and IPv6 datagrams. An AH is normally inserted after an IP header and before the other information being authenticated. The AH is a mechanism for providing strong integrity and authentication for IP datagrams. It might also provide non-repudiation, depending on which cryptographic algorithm is used and how keying is performed.

The Internet Draft "IP Encapsulating Security Payload (ESP)," Stephen Kent (BBN Corp), Randall Atkinson (@Home Network), 30 May 1997, draft-ietf-ipsec-esp-04.txt, discusses a mechanism for providing integrity and confidentiality to IP datagrams. In some circumstances, depending on the encryption algorithm and mode used, it can also provide authentication to IP datagrams. Otherwise, the IP AH may be used in conjunction with ESP to provide authentication. The mechanism works with both IPv4 and IPv6.

RFC 2104, "HMAC: Keyed-Hashing for Message Authentication," February 1997, H. Krawczyk (IBM), M. Bellare (UCSD), R. Canetti (IBM). This document describes HMAC, a mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function, e.g., MD5, SHA-1, in combination with a secret shared key. The cryptographic strength of HMAC depends on the properties of the underlying hash function.

RFC 1829, "The ESP DES-CBC Transform," P. Karn (Qualcomm), P. Metzger (Piermont), W. Simpson (Daydreamer), August 1995. The Encapsulating Security Payload (ESP) provides confidentiality for IP datagrams by encrypting the payload data to be protected. This specification describes the ESP use of the Cipher Block Chaining (CBC) mode of the US Data Encryption Standard (DES) algorithm (FIPS-46, FIPS-46-1, FIPS-74, FIPS-81). All implementations that claim conformance or compliance with the ESP specification must implement this DES-CBC transform.

The Domain Name System (DNS) has become a critical operational part of the Internet infrastructure yet it has no strong security mechanisms to assure data integrity or authentication. IETF RFC-2065, "DNS Security Extensions," D. Eastlake, C. Kaufman, January 1997, describes extensions to the DNS that provide these services to security aware resolvers or applications through the use of cryptographic digital signatures. These digital signatures are included in secured zones as resource records. Security can still be provided even through non-security aware DNS servers in many cases. The extensions also provide for the storage of authenticated public keys in the DNS. This storage of keys can support general public key distribution service as well as DNS security.

The IETF Draft, "Internet Security Association and Key Management Protocol (ISAKMP)," Douglas Maughan, Mark Schertler, Mark Schneider, Jeff Turner, 21 February 1997, draft-ietf-ipsec-isakmp-07.txt, describes a protocol utilizing security concepts necessary for establishing Security Associations (SAs) and cryptographic keys in an Internet environment. It is expected that the IETF will adopt this protocol as the Internet standard for key and security association management for IPv6 security.

The IETF Draft, "The Resolution of ISAKMP with Oakley," D. Harkins, D. Carrel (Cisco Systems), February 1997, draft-ietf-ipsec-isakmp-oakley-03.txt, describes a proposal for using the Oakley Key Exchange Protocol in conjunction with ISAKMP to obtain authenticated keying material for use with ISAKMP, and for other security associations such as AH and ESP for the IETF IPsec Domain of Interpretation (DOI). ISAKMP provides a framework for authentication and key exchange but does not define them. ISAKMP is designed to be key exchange independent; that is, it is designed to support many different key exchanges. Oakley describes a series of key exchanges – called "modes" – and details the services provided by each (e.g., perfect forward secrecy for keys, identity protection, and authentication).

The Internet Draft, "The Internet IP Security Domain of Interpretation for ISAKMP," Derrell Piper (Cisco Systems), 28 February 1997, draft-ietf-ipsec-ipsec-doi-02.txt, details the Internet IP Security DOI, which is defined to cover the IP security protocols that use ISAKMP to negotiate their security associations. The ISAKMP defines a framework for security association management and cryptographic key establishment for the Internet. This framework consists of defined exchanges and processing guidelines that occur within a given DOI.

Two IEEE LAN security standards are emerging: IEEE 802.10, IEEE Standards for Local and Metropolitan Area Networks (MANs): Interoperable LAN/MAN Security (SILS), 1992, discusses services, protocols, data formats and interfaces to allow IEEE 802 products to interoperate, and discusses authentication, access control, data integrity, and confidentiality; IEEE 802.10a, Standard for Interoperable LAN Security – The Model, Draft January 1989, shows the relationship of SILS to OSI and describes required interfaces. IEEE 802.10b, Secure Data Exchange, 1992, is incorporated in IEEE 802-10, and deals with secure data exchange at the data link layer.

2.6.3.4 Information Modeling, Metadata, and Information Security Standards

There are no emerging standards in this area at this time.

2.6.3.5 Human-Computer Interface Security Standards

Refer to Section 2.6.3.2.1.1 for information pertaining to the Common Criteria Protection Profiles emerging standard that is expected to replace DoD 5200.28-STD.

Refer to Section 2.6.3.3.1.1.2 for information pertaining to FIPS PUB 196, Entity Authentication Using Public Key Cryptography, 18 February 1997.